Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	WC Docket No. 18-89
Threats to the Communications Supply	)	
Chain Through FCC Programs	)	
	)	

COMMENTS OF USTELECOM – THE BROADBAND ASSOCIATION

Michael D. Saperstein, Jr.

USTelecom – The Broadband Association
601 New Jersey Ave. NW
Suite 600
Washington, DC 20001

June 1, 2018

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89
	)	
	)	
	)	

COMMENTS OF
USTELECOM – THE BROADBAND ASSOCIATION

USTelecom — The Broadband Association (USTelecom)[1] submits these comments in response to the Federal Communications Commission's (Commission) Notice of Proposed Rulemaking[2] proposing to prevent federal Universal Service Fund (USF) recipients from using USF funds "to purchase equipment or services from any communications equipment or service providers identified as posing a national security risk to communications networks or the communications supply chain."[3] USTelecom supports the Commission's effort through this *Notice* to highlight and mitigate potential risks in the communications supply chain as a part of ongoing federal risk management efforts.

I. Introduction and Summary

USTelecom agrees that USF funds should not support those that seek to harm American national security interests. USTelecom members have a broad range of experience combatting threats to the communications network supply chain across numerous federal initiatives.

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives – all providing advanced communications service to both urban and rural markets.

[2] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Notice of Proposed Rulemaking, FCC 18-42 (Apr. 18, 2018) (*Notice*).

[3] *Id.* at para. 2.

USTelecom members also comprise a large proportion of the total USF funding recipients, particularly of the High-Cost Support Program. Our collective experience with the supply chain and USF programs leads us to validate the Commission's "specific, but important, supporting role,"[4] as the steward of American USF ratepayer resources. We agree with Chairman Pai that, "[t]o be sure, the FCC doesn't have the authority or the capacity to solve this problem alone. But it does have a role to play in meeting this challenge."[5]

As the *Notice* demonstrates, there is a substantial body of evidence suggesting that risks to the confidentiality, integrity, and authenticity of the nation's communications networks emanate from the use of certain providers of network equipment and services, including Huawei, ZTE, and Kaspersky Labs.[6] Accordingly, it is entirely appropriate that the Commission seek to limit USF recipients from purchasing such equipment and services so long as the Commission adopts fundamental tenets in its approach:

- Balancing the national security and commercial interests intertwined with the supply chain require substantial and continual federal government coordination. The Commission must closely coordinate all of its actions in this field across the federal government.
- The Commission is not in the best position to determine the threats to and vulnerabilities of the communications supply chain; it should rely heavily on other federal agencies, particularly the Department of Homeland Security (DHS), to make its determinations about appropriate prospective restrictions and remedial measures where suspect equipment exists today.
- Any restrictions on the use of USF funding should be prospective, taking into account existing equipment and a level playing field.
- The Commission should confine the scope of any rule to apply only to equipment and services funded through the Universal Service Fund in order to stay clearly within the bounds of its legal authority.

[4] *Id.* at para 2.

[5] *Id.*, Statement of Chairman Ajit Pai at 1.

[6] *Id.* at paras. 3-6.

II. FCC Action on Supply Chain Issues Cannot Take Place in a Vacuum: Federal Coordination is Essential.

USTelecom recognizes that today's cyber ecosystem is a highly complex and dynamic universe consisting of a global set of diverse stakeholders. Developing and promoting effective prevention, response and recovery capabilities, and working in partnership with all stakeholders in the internet ecosystem, is a top priority for USTelecom members.

USTelecom and its members play a leading role in organizing sector advocacy with other trade associations and various government partnership councils and committees. We work closely with numerous government and industry stakeholders in a broad variety of cyber infrastructure resilience initiatives.[7] We have partnerships within DHS's Office of Cybersecurity and Communications,[8] and the DHS Office of Infrastructure Protection[9] designed to promote greater coordination and collaboration across critical infrastructure sectors and increase education and awareness efforts related to cybersecurity threats, information sharing, and incident response. USTelecom also works with the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST) under the Department of Commerce, and is an active participant in the Commission's Communications Security, Reliability and Interoperability Council (CSRIC),[10] which develops best practices through collaborative and voluntary efforts with cybersecurity and technology professionals. In

[7] *See generally* USTelecom, Filings-Cybersecurity, https://www.ustelecom.org/issues/filings/1 (last visited June 1, 2018) (presenting a representative sampling of USTelecom's engagement in cybersecurity matters across numerous branches of the federal government).

[8] DHS, Office of Cybersecurity and Communications, https://www.dhs.gov/office-cybersecurity-and-communications (last visited June 1, 2018).

[9] DHS, Office of Infrastructure Protection, https://www.dhs.gov/office-infrastructure-protection (last visited June 1, 2018).

[10] FCC, Communications Security, Reliability and Interoperability Council, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited June 1, 2018).

particular, USTelecom was an active participant in CSRIC IV's effort to adapt the general NIST Cyber Risk Management Framework to the communications sector.[11]

USTelecom members' broad range of experience extends to combatting threats to the communications network supply chain across numerous federal initiatives and frames our viewpoint that a "whole of government" approach is particularly necessary in the context of supply chain risk management.

A. Federal Communications Supply Chain Activities and Initiatives are Proliferating

The Commission's efforts to identify and mitigate supply chain risk in the communications sector are just one initiative in an increasingly complex federal landscape addressing the problem; the Commission must stay fully informed of, and engaged with, other federal entities that are also undertaking efforts to address risk in the communications supply chain. The *Notice* accurately describes the state of federal concern that existed when the Commission was considering the draft of the *Notice*,[12] but much has changed even in the short timeframe since then that must inform the Commission's role and responsibilities.

Beginning on April 16, 2018, the day before the Commission voted to approve the *Notice*, the following federal activities related to communications supply chain risk have occurred:

- April 16, 2018: The Commerce Department barred American suppliers from exporting equipment to ZTE for seven years in a move that stemmed from ZTE's previous violations of U.S. sanctions for selling to Iran and North Korea.[13]

---

[11] CSRIC, Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report (2015) https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[12] *See Notice* at paras 3-6.

[13] David J. Lynch, *U.S. Companies Banned from Selling to China's ZTE Telecom Maker*, Wash. Post (Apr. 16, 2018) available at https://www.washingtonpost.com/news/business/wp/2018/04/16/u-s-companies-banned-from-selling-to-chinas-zte-telecom-maker/?noredirect=on&utm_term=.ed374e90bad6.

- April 16, 2018: NIST released an update to its Cybersecurity Framework that included a section on "managing cybersecurity within the supply chain."[14]

- April 19, 2018: The U.S.-China Economic and Security Review Commission released a report titled *Supply Chain Vulnerabilities in U.S. Federal Information and Communications Technology*, which examines vulnerabilities and makes recommendations for supply chain risk management. The cited threats include Huawei and ZTE, but also other companies beyond those included in the FCC's *Notice*. [15]

- May 2, 2018: The Pentagon banned U.S. military bases from selling Huawei and ZTE phones.[16]

- May 4, 2018: The House Armed Services Committee circulated a draft of the National Defense Authorization Act (NDAA) that includes significant findings implicating Huawei and ZTE equipment as security risks.[17] The bill would, among other restrictions related to Huawei and ZTE usage, prohibit federal agencies from contracting with "an entity that uses any equipment, system or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system."[18]

- May 7, 2018: The Department of Homeland Security (DHS) briefed the communications sector on upcoming efforts to conduct a general and specific communications supply chain risk assessment.[19]

- May 9, 2018: ZTE announced it would end "major operating activities" due to the Commerce Department barring U.S. suppliers from exporting to ZTE.[20]

---

[14] NIST, NIST Releases Version 1.1 of its Popular Cybersecurity Framework (Apr. 16, 2018) https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

[15] Interos Solutions, Inc., prepared for the U.S.-China Economic and Security Review Commission, Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology at 14-15 (Apr. 2018), https://www.uscc.gov/sites/default/files/Research/Interos_Supply%20Chain%20Vulnerabilities%20from%20China%20in%20U.S.%20Federal%20ICT_final.pdf.

[16] Hamza Shaban, *Pentagon Tells U.S. Military Bases to Stop Selling ZTE, Huawei Phones*, Wash. Post (May 2, 2018) available at https://www.washingtonpost.com/news/the-switch/wp/2018/05/02/pentagon-tells-u-s-military-bases-to-stop-selling-zte-huawei-phones/?utm_term=.c366659dca06.

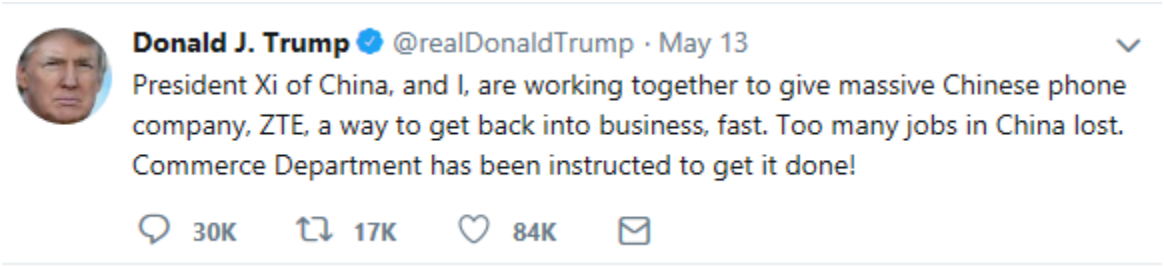
[17] National Defense Authorization Act for FY 2019, H.R. 5515, 115th Cong. (2018).

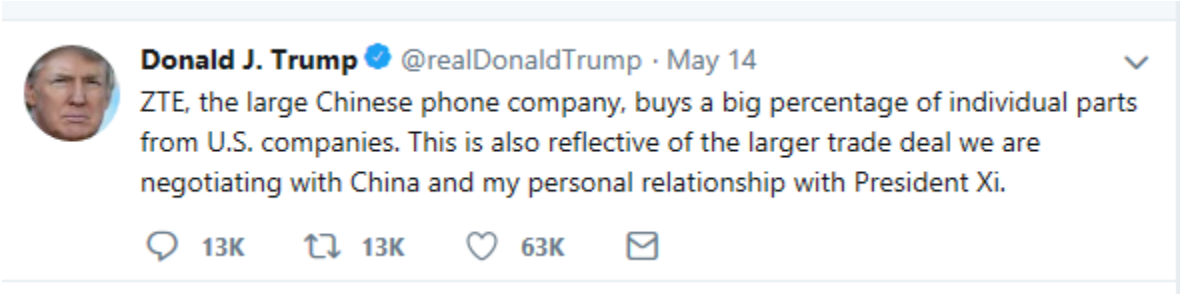
[18] *Id.* at § 880(b)(1).

[19] Tim Starks, *DHS Tackles Systemic Risk, Supply Chain Threats*, Politico (May 7, 2018) available at https://www.politico.com/newsletters/morning-cybersecurity/2018/05/07/dhs-tackles-systemic-cyber-risk-supply-chain-threats-205953.

[20] Hamza Shaban, *ZTE Ends Major Operations After U.S. Export Ban*, Wash. Post (May 10, 2018) available at https://www.washingtonpost.com/news/the-switch/wp/2018/05/10/zte-ends-major-operations-after-u-s-export-ban/?utm_term=.56425bfaa98c.

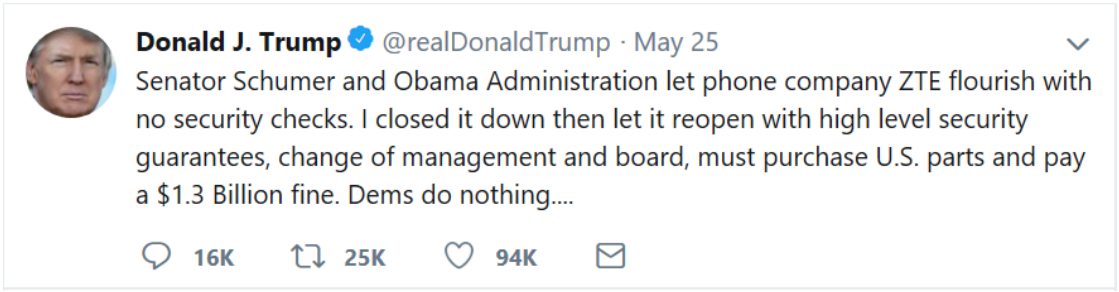
- May 13-14, 2018: President Trump issues the following tweets:[21]





- May 16, 2018: The House Energy and Commerce Committee held a hearing on communications supply chain issues titled, "Telecommunications, Global Competitiveness, and National Security."[22]

- May 25, 2018: President Trump issues this tweet: [23]



- May 27, 2018: "Rubio, in challenge to Trump, suggests Congress will act against ZTE."[24]

---

[21] Trump, Donald J., Twitter Post. May 13-14, 2018. https://twitter.com/realDonaldTrump.

[22] *See* House Energy & Commerce Committee Subcommittee on Internet and Technology, Subcommittee on Internet & Technology, May 16, 2018 hearing, "Telecommunications, Global Competitiveness and National Security."

[23] Trump, Donald J., Twitter Post. May 25, 2018. https://twitter.com/realDonaldTrump.

[24] Karoun Demirjian, *Rubio, in Challenge to Trump, Suggests Congress Will Act Against ZTE*, Wash. Post, available at https://www.washingtonpost.com/powerpost/rubio-in-challenge-to-trump-suggests-congress-will-act-against-zte/2018/05/27/5bff13e8-61cb-11e8-a768-ed043e33f1dc_story.html?utm_term=.084d082a9eaf.

Given the constant stream of events affecting federal communications supply chain policy, the Commission must be involved in a coordinated fashion across the federal government in order to make an informed decision on how to best identify meaningful supply chain risks and the appropriate actions to mitigate them. Each of these events involves an important, but different, vector of federal supply chain oversight that could affect how the Commission determines which companies USF recipients are barred from using in the supply chain. While the Commission was commendably at the forefront of federal initiatives related to supply chain security risk, it must view its proposals in the context of a dynamic and complicated environment that includes concerns regarding security, commerce, and American global competitiveness. Failure to do so could lead to the Commission either undermining other federal interests, or to not representing the latest developments in supply chain risk and leaving a hole that affects the security of our communications networks.

B. The Commission Should Make Use of the DHS Supply Chain Risk Assessment to Inform its Decisions in this Proceeding

The most important issue that the Commission must decide in this proceeding is how it will identify both the companies, and the types of equipment and services produced by those companies, that constitute a national security risk. While USTelecom members support the Commission's targeted approach in concept, the identification aspect of the Commission's proposal invokes substantial issues of business certainty. The private sector entities charged with deploying U.S. communications networks generally make supply chain decisions with long lead times and at scale, based upon a variety of factors. Any Commission bar on the use of a network or services vendor will have major ramifications that affect the supply and demand balance, which is particularly the case in a concentrated industry of communications network suppliers. [25]

[25] Olof Swahnberg and Eric Auchard, *ZTE Woes May Boost Network Rivals Ericsson and Nokia*, Reuters (Apr. 19,

Such disruptions go not only to the unit pricing of equipment and services, but also can affect delivery dates and deployment schedules if product demand shifts suddenly. The potential market effects of the Commission's actions are true of the vendors in question today (i.e., Huawei, ZTE, Kaspersky Labs) but USTelecom Members are also concerned about the effects on potential vendors that the Commission may identify as a national security threat in the future, making a sound process essential.

Supply chain risk lives at the intersection of vulnerabilities and threats; the FCC is not in a position to actively determine either on its own. The Commission has not previously demonstrated an independent capability to examine and evaluate technical vulnerabilities in the communications supply chain. As the *Notice* acknowledges, its primary mechanism for establishing norms with respect to security is the CSRIC, "which is charged with providing recommendations to ensure the security and reliability of the nation's communications systems, including telecommunications, media and public safety networks."[26] USTelecom and its members are active supporters of CSRIC, but given CSRIC's timing, schedule, and composition, it lacks the ability to undertake the substantial and continual effort of identifying how vulnerabilities may enter the supply chain throughout the ecosystem. Similarly, supply chain threat information, which describes how known vulnerabilities can be leveraged by those seeking to do harm, generally comes from the intelligence community in a classified manner. The Commission is currently ill-suited to synthesize the in-depth and continuous vulnerability discovery and threat information required to determine which entities and which pieces of specific equipment pose national security threats.

2018) https://www.reuters.com/article/us-usa-china-zte-rivals/zte-woes-may-boost-network-rivals-ericsson-and-nokia-idUSKBN1HQ1YK.

[26] *Notice* at para. 9.

Further, the Commission, as an independent agency bound by the Administrative Procedure Act,[27] may not be at the forefront of the complex and rapid decision-making process that involves significant inputs from various components of the Executive branch (Department of Commerce, Department of Defense, Department of Homeland Security, etc.). As demonstrated above with the supply chain activity over the past six weeks since the Commission approved the *Notice*, the pace at which decisions are made with respect to commerce and national security outpace the Commission's ability to effectively develop and maintain a timely and consistent list of equipment that poses a national security risk.

DHS, as the entity responsible for managing all threats across federal networks and critical infrastructure,[28] has recently indicated that it will be conducting two communications supply chain risk assessments, one general and one that is more specific and comprehensive.[29] Both assessments are projected to be completed in the relatively near future. While we do not suggest that the FCC should transfer its role in ensuring the appropriate use of USF funding in the supply chain to DHS, it should at least defer its action in this proceeding until DHS has completed its evaluations of what the supply chain threats and vulnerabilities are in the communications networks.

Further, USTelecom urges the Commission to actively participate in DHS's comprehensive telecommunications supply chain risk assessment as much as possible.[30] We

---

[27] Administrative Procedure Act, 5 U.S.C. § 500 *et seq*. *See also* FCC, Rulemaking Process, https://www.fcc.gov/about-fcc/rulemaking-process (last visited June 1, 2018).

[28] *See* "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience," rel. Feb. 12, 2013, available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (PPD 21).

[29] *See supra* n. 19.

[30] The FCC is a member of the Communications Sector Government Coordinating Council. "Government Coordinating Councils (GCCs) are formed as the government counterpart for each Sector Coordinating Council

believe that this collaboration will allow the agencies to develop a joint understanding of the risk, avoid duplication of efforts, and ensure productive outputs for both government and industry. The DHS process has two substantial benefits beyond any process that the Commission could undertake.

First, due to DHS's broad mandate, it has the ability to effectively evaluate and incorporate the information technology (IT) community,[31] which is responsible for much of the software and hardware that comprise the nation's communications networks, in its risk assessment in a meaningful way. As the Commission raises specific questions related to what types of software should be implicated by its rule, the DHS venue provides an opportunity for a more fulsome exploration of the issue.[32]

Second, DHS can offer companies the ability to participate in a risk assessment under the auspices of the DHS Protected Critical Infrastructure Information (PCII) program. By statute[33] and regulation,[34] information that is determined to be PCII cannot: (1) be disclosed through a Freedom of Information Act request (nor similar state/local disclosure laws); (2) be disclosed in civil litigation; and (3) be used for a regulatory purpose.[35] The purpose of the PCII program is to

(SCC) to enable interagency and cross-jurisdictional coordination. The GCCs are comprised of representatives from across various levels of government (federal, state, local, or tribal), as appropriate to the operating landscape of each individual sector. Each GCC is chaired by a representative from the designated sector-specific agency with responsibility for ensuring appropriate representation on the council and providing cross-sector coordination with state, local, tribal, and territorial (SLTT) governments. The Department of Homeland Security Assistant Secretary for Infrastructure Protection or a designee co-chairs all GCCs. The GCC coordinates strategies, activities, policy, and communications across governmental entities within each sector." DHS, Government Coordinating Councils, https://www.dhs.gov/gcc (last visited June 1, 2018).

[31] DHS is also the Sector Specific Agency for the Information Technology Sector. *See PPD 21*, *supra* n. 28.

[32] *See Notice* at para. 15, ("[S]hould the rule cover all software or only software that manages the communications network or devises used on the network?)."

[33] Critical Information Act of 2002, 6 U.S.C. §§131 *et seq*.

[34] 6 C.F.R. pt. 29.

[35] DHS, Protected Critical Infrastructure Information Program, Jan. 2017,

better enable collaboration between the private sector and DHS by creating a venue in which "infrastructure information voluntarily shared with DHS could be used for homeland security purposes, while simultaneously protecting the sensitive information from public disclosure."[36] Under this program, communications network providers and IT providers alike will feel more confident in participating in a process that necessarily involves divulging very sensitive information about potential vulnerabilities in their products.

C. The DHS Supply Chain Risk Assessment Process Should Determine Prohibited Equipment and Inform Many of the Commission's More Challenging Questions Regarding the Scope of Prohibition

The results of the risk assessment should be used to develop a list of communications equipment or service providers that raise national security concerns, which could be held and maintained by DHS based on specific criteria. The Commission asks a number of important questions related to what types of equipment and services should be covered by its proposed rule[37] but it would be premature to answer them in advance of the DHS supply chain risk assessment. The very purpose of DHS's supply chain inquiry is to analyze communications equipment and services based on specific threats, vulnerabilities and entities at risk. Accordingly, one would expect the DHS process to answer key questions like whether the proposed rule should be limited to "equipment and services that relate to the management of a network, data about the management of a network, or any system the compromise or failure of which could disrupt the confidentiality, availability, or integrity of a network."[38] Answers to such questions need to be

https://www.dhs.gov/sites/default/files/publications/pcii-fact-sheet-2017-508.pdf.

[36] *Id.*

[37] *Notice* at para 15.

[38] *Id.*

developed using a unified federal approach informed by the intelligence community—not one based upon individualized experiences as the FCC's comment process necessarily evokes.

An advantage of the Commission directly participating in the DHS risk assessment process is that the Commission can help to assure that the DHS process answers the questions that the Commission needs to move forward with its proposed rule. To the extent possible, the Commission should coordinate to ensure that its questions related to what products and services should be barred from USF use are included within the scope of DHS's targeted supply chain risk assessment. Such effort will involve comprehensively identifying all manufacturers, equipment, products, software and services that may be manipulated by various adversaries. For example, the Commission should work with DHS to examine whether equipment produced by Huawei/ZTE that lacks the capacity to route or redirect traffic, or that has no visibility into the packets or data it transmits constitutes the same type of threat to the supply chain as other "smart" equipment, which may pose a more instant and impactful threat. It is essential to properly scope the risks and their correlation with specific types of equipment, products and services in order to appropriately tailor measures taken to protect the nation's networks and services now and in the future.

Absent the DHS risk assessment, USTelecom is unaware of any existing process or method under which supply chain risk analysis results in a certification that a particular vendor or piece of equipment is not a supply chain risk. Such an undertaking would be extremely challenging given the complexity and variation of the equipment, as well as "gray market equipment,"[39] used in communications networks. It is unlikely that the FCC could convene an

[39] "Gray market equipment" refers to components of network equipment that are purchased from an entity other than the manufacturer of that equipment, typically because the original manufacturer no longer sells those components. For example, a carrier may purchase cards for a router from a third-party vendor after the router manufacturer stops support of that model.

advisory group or voluntary industry panel to achieve the same result due to the generally classified nature of threat information, as well as reluctance of the private sector to share their known vulnerabilities. For that reason, meaningful supply chain risk analysis is properly situated within DHS. Also, DHS has the ability to influence supply chain decisions across the internet ecosystem; security concerns related to equipment and services cannot be effectively addressed if applied only to communications networks.

Alternatively, to the extent that DHS is unable to meaningfully coordinate, develop, and maintain a list of prohibited vendors, the FCC could look to external federal sources to develop a list of prohibited vendors, equipment and services. While not as precise a tool, legislation such as the National Defense Authorization Act (NDAA) can be useful in providing a public bright line standard of conduct upon which the FCC can base its decisions on what it will fund. The difficulty with relying on such a legislative standard is that the legislation is subject to variations from year to year without a formal regulatory process to explain changes from one iteration to another. In any case, the list would need to be premised on the intelligence and experience from experts in the intelligence community and the Department of Defense, and made available in a public forum.

III. There Are Practical Considerations that the Commission Can Evaluate Now to Appropriately Tailor its Proposed Rule

While the specific scope of the equipment and services at issue should be defined after the Commission participates in the DHS supply chain risk assessment, there are practical considerations that the Commission should consider now in order to improve its underlying rule proposal.

A. Any restrictions on the use of USF funding should be prospective, taking into account existing equipment and a level playing field.

In order to avoid second-guessing network decisions made in good faith and in accordance with existing USF rules, the Commission should only apply its rules prospectively. In this manner the Commission can avoid unnecessary legal entanglements associated with retroactively directing how funding should have been spent. To the extent that the DHS risk assessment process recommends remediation or removal of existing equipment, the Commission should consider adopting a phase-in of the effective dates to address the existing equipment that poses the most risk first (e.g., equipment with routing capabilities). In general, network providers with existing contracts should be allowed to continue the management and maintenance of existing equipment over the component's reasonable lifecycle.

However, the Commission need not set a far-removed effective date for any rules it chooses to adopt on the purchase of new equipment related to Huawei, ZTE or Kaspersky Labs, particularly for communications network providers (differentiated from, for example, schools, libraries and rural healthcare providers).[40] USF recipients, by virtue of this *Notice* and all of the numerous events taking place across the federal government related to supply chain issues, should be on notice that their continued use of these vendors may have national security implications that could affect their ability to receive federal funding. It is commonly understood that equipment from these providers is often available at costs substantially below that of other equipment vendors. Despite this, many USTelecom members have made difficult choices to purchase the more expensive equipment in order to avoid security risks. Particularly as future USF support becomes more predicated on a market-based, auction methodologies, the Commission should be aware of the tension between its national security goals and its goal to

[40] *Notice* at para. 17.

maximize fund efficiency if network providers continue taking advantage of reduced-cost equipment that carries security risks in their bids. While this may drive down the cost of service in the short term and allow them to win their respective auction, the long-term costs to the country associated with knowingly installing suspect equipment now are difficult to justify.

B. The Commission Should Not Extend the Scope of the Rule Beyond Prohibitions Related to USF Funding

The Commission should confine the scope of any rule to apply only to equipment and services funded through the Universal Service Fund in order to stay clearly within the bounds of its legal authority.[41] USTelecom agrees with the Commission's analysis that section 254 of the Communications Act provides the Commission with authority to establish public interest principles, such as national security, that guide the rules it establishes for use of USF funding.[42] However, USTelecom does not agree that section 201(b) gives the Commission explicit authority beyond giving meaning to its section 254 authority in this case.

The Commission lacks authority to adopt its greatly expanded proposal to "consider actions targeted not only at the USF-funded equipment or services of those companies, but also non USF-funded equipment or services produced or provided by those companies that might pose the same or similar national security threats to the nation's communications networks."[43] All of the existing models that the Commission cites to address supply chain issues—the NDAA, the Spectrum Act, pending legislation and GSA databases—make use of a procurement model approach to incent and curb behavior.[44] Where an entity wants to do business with the government, it must follow the standards set in accordance with governmental priorities; these

[41] *See id.* at para. 31.

[42] *Id.* at para. 35.

[43] *Id.* at para. 31.

[44] *Id.* at paras. 20-23.

models do not purport to ban disfavored vendors throughout the United States. Section 201(b), despite providing the authority to promulgate "such rules and regulations as may be necessary in the public interest to carry out the provisions of th[e] Act,"[45] cannot be read to provide the Commission with such expansive authority to effectuate a total ban of commerce, lest it become a limitless grant of authority over anything related to communications. Further, as a practical matter, for the Commission to adopt this approach it must apply it across the entire communications ecosystem—including the IT sector—for it to be of any value in an interconnected world. The *Notice* does not attempt to establish authority to do so and the Commission cannot proceed accordingly without a serious explanation of its proposed authority in this area.

IV. Conclusion.

USTelecom supports the Commission's efforts to exercise good stewardship over its USF spending but emphasizes the need for a coordinated, "whole of government" approach to determining the entities and equipment types that constitute communications supply chain risks.

Respectfully submitted,

By: _____

Michael Saperstein
USTelecom Association
601 New Jersey Avenue, N.W.
Suite 600
Washington, D.C. 20001
(202) 326-7300

June 1, 2018

[45] 47 U.S.C. § 201(b).